Acta Sci. Math., 45 (1983), 151—160

Série de Poincaré et systèmes de paramètres pour les invariants des formes binaires

J. DIXMIER

Pour le 70-ième anniversaire du Professeur Béla Sz.-Nagy

1. Introduction. Soient G un groupe, V un espace vectoriel complexe de dimension finie, $\mathbf{C}[V]$ l'algèbre des fonctions complexes polynomiales sur V, ϱ une représentation linéaire de G dans V, $\mathbf{C}[V]^G$ la sous-algèbre de $\mathbf{C}[V]$ formée des éléments $\varrho(G)$-invariants. Soient $\mathbf{C}[V]_n^G$ l'ensemble des éléments de $\mathbf{C}[V]^G$ qui sont homogènes de degré n, et $d_n = \dim \mathbf{C}[V]_n^G$. La série de Poincaré de l'algèbre graduée $\mathbf{C}[V]^G$ est $F(z) = \sum_{n \geqq 0} d_n z^n$.

Supposons désormais que G soit un groupe algébrique réductif et que la représentation ϱ soit rationnelle. Soit $(p_1, \ldots, p_r)$ un système de paramètres homogènes dans $\mathbf{C}[V]^G$ (il en existe). Alors $\mathbf{C}[V]^G$, considéré comme module sur $\mathbf{C}[p_1, \ldots, p_r]$, admet une base $(q_1 = 1, q_2, q_3, \ldots, q_s)$ formée d'éléments homogènes (cf. par exemple [7]). Si l'on pose $\deg p_i = d_i$, $\deg q_j = e_j$, on a donc

$$F(z) = \frac{z^{e_1} + z^{e_2} + \ldots + z^{e_s}}{(1 - z^{d_1})(1 - z^{d_2}) \ldots (1 - z^{d_r})}.$$

Réciproquement, supposons que $F(z)$ se mette sous la forme

$$F(z) = \frac{z^{e'_1} + z^{e'_2} + \ldots + z^{e'_t}}{(1 - z^{d'_1})(1 - z^{d'_2}) \ldots (1 - z^{d'_r})}$$

où $e'_1, \ldots, e'_t, d'_1, \ldots, d'_r$ sont des entiers > 0 (r est nécessairement l'ordre du pôle 1). Existe-t-il un système de paramètres homogènes de degrés $d'_1, \ldots, d'_r$? Un contre exemple a été obtenu par R. STANLEY [7], 3.8, dans lequel G est un groupe fini. Nous allons construire un contre-exemple dans lequel $G = SL(2, \mathbf{C})$.

Avec les notations ci-dessus, la borne inférieure de s pour tous les systèmes de paramètres homogènes de $\mathbf{C}[V]^G$ a été appelée dans [2] la *complexité* de $\mathbf{C}[V]^G$;

Reçu le 22 juin, 1982.

ce nombre fournit une manière de mesurer la «distance» de $\mathbf{C}[V]^G$ à une algèbre de polynômes. Dans le contre-exemple annoncé, nous calculerons cette complexité.

Désormais, on prend $G=SL(2,\mathbf{C})$. Soit V_d l'espace des formes binaires de degré d à coefficients complexes, dans lequel G opère canoniquement par une représentation irréductible ϱ_d (on a $\dim V_d=d+1$). Soit c_d la complexité de $\mathbf{C}[V_d]^G$. T. A. SPRINGER a obtenu [6] l'évaluation $c_d \geqq \alpha d^{-9/2}2^d$ où α est un nombre >0 indépendant de d. La démonstration de Springer utilise des calculs assez délicats concernant la série de Poincaré; mais, concernant les degrés des p_j, Springer n'utilise que l'inégalité évidente $\deg p_j \geqq 2$; en conservant la méthode de Springer, mais en évaluant ces degrés de manière plus détaillée, nous prouverons que, si A est un nombre $<1/2$, on a $c_d \geqq \exp(Ad\log d)$ pour d assez grand. La démonstration utilise un théorème sur la répartition des nombres premiers.

Première partie

2. Soient $V=V_5\oplus V_1$, $\varrho=\varrho_5\oplus\varrho_1$. La décomposition $V=V_5\oplus V_1$ définit une bigraduation $(\mathbf{C}[V]^G_{m,n})_{m\geqq 0,\,n\geqq 0}$ de $\mathbf{C}[V]^G$. Soit $a_{mn}=\dim \mathbf{C}[V]^G_{m,n}$. La série de Poincaré de l'algèbre bigraduée $\mathbf{C}[V]^G$ est $\Phi(z,z')=\sum_{m,n\geqq 0} a_{mn}z^m z'^n$. Comme $\mathbf{C}[V]^G$ s'identifie à l'algèbre des covariants d'une forme binaire de degré 5, on trouve la valeur de $\Phi(z,z')$ dans [8], p. 224.

Comme dans l'introduction, graduons maintenant $\mathbf{C}[V]^G$ par le degré total. Sa série de Poincaré est $F(z)=\Phi(z,z)$. Utilisant [8], on trouve

$$F(z)=\frac{1-z^2+z^6+5z^8-3z^{10}+3z^{12}-5z^{14}-z^{16}+z^{20}-z^{22}}{(1-z^2)(1-z^4)^2(1-z^6)^2(1-z^8)}.$$

Le numérateur est divisible par $1-z^2$, d'où

$$F(z)=\frac{1+z^6+6z^8+3z^{10}+6z^{12}+z^{14}+z^{20}}{(1-z^4)^2(1-z^6)^2(1-z^8)}. \tag{1}$$

On vérifie facilement que l'écriture (1) est la forme irréductible de $F(z)$. Comme tous les coefficients du numérateurs sont $\geqq 0$, cette forme de $F(z)$ est du type considéré dans l'introduction. Comme elle est irréductible, c'est l'unique écriture minimale de $F(z)$ au sens de [2].

3. Lemme. *Soit* $\varphi=ax^5+5bx^4y+10cx^3y^2+10dx^2y^3+5exy^4+fy^5$ *une forme binaire de degré* 5. *Soit* ψ *le transvectant* $(\varphi,\varphi)_4$. *On a*

$$\frac{1}{2}\psi=(ae-4bd+3c^2)x^2+(af-3be+2cd)xy+(bf-4ce+3d^2)y^2. \tag{2}$$

Les conditions suivantes sont équivalentes:

(i) φ *a une racine d'ordre* $\geqq 4$ *en* x/y;

(ii) $\psi=0$.

La formule (2) est très facile. Pour prouver (i)$\Rightarrow$(ii), on peut, par action de $SL(2, \mathbf{C})$, se ramener au cas où $\varphi=ax^5+5bx^4y$; alors $\psi=0$ d'après (2). Supposons maintenant $\psi=0$, et prouvons (i), qui est d'ailleurs un casparticulier de P. GORDAN, *Vorlesungen über Invariantententheorie*, 1885, p. 204.

Par action de $SL(2, \mathbf{C})$, on se ramène au cas où $f=0$. La condition $\psi=0$ se traduit alors par $ae-4bd+3c^2=-3be+2cd=-4ce+3d^2=0$. Si $e=0$, on trouve $d=0$, $c=0$, donc (i) est vérifié. Supposons $e\neq 0$. Par action de $SL(2, \mathbf{C})$, on peut, sans perdre les conditions précédentes, supposer que $d=0$. Alors, on trouve $c=0$, $b=0$, $a=0$, donc (i) est encore vérifié.

4. Soit $(\varphi, \varphi')\in V_5\oplus V_1=V$, avec

$$\varphi=ax^5+5bx^4y+10cx^3y^2+10dx^2y^3+5exy^4+fy^5,\ \varphi'=a'x+b'y.$$

L'algèbre $\mathbf{C}[V]^G$ s'identifie à l'algèbre des covariants de φ. On a donc en [4], p. 131, une table de générateurs de $\mathbf{C}[V]^G$. Posons

$$\psi_1=\frac{1}{2}(\varphi, \varphi)_2\in V_{6;\,2,0},\quad \psi_2=\frac{1}{2}(\varphi, \varphi)_4\in V_{2;\,2,0},\quad \psi_3=(\varphi, \psi_1)_1\in V_{9;\,3,0}.$$

(La notation $\omega\in V_{i;\,j,k}$ signifiera que ω est une forme homogène de degré i en x et y, dont les coefficients sont homogènes de degré j en $a, b, \ldots, f$, et de degré k en a', b'.) Alors $(\psi_2, \psi_2)_2$ est un scalaire qui dépend de φ, disons $p_1(\varphi)$, où p_1 est une fonction polynomiale homogène de degré 4 de $a, b, \ldots, f$. On a $p_1\in\mathbf{C}[V_5]^G_4$. Nous considérerons p_1 comme une fonction polynomiale bihomogène sur V, de bidegré (4, 0): $p_1\in\mathbf{C}[V]^G_{4,0}$.

Définissons de même $p_2\in\mathbf{C}[V]^G_{8,0}$ et $p_3\in\mathbf{C}[V]^G_{12,0}$ par

$$p_2(\varphi)=(\psi_2^3, \psi_1)_6,\quad p_3(\varphi)=(\psi_2^5, \varphi^2)_{10}.$$

Les fonctions p_1, p_2, p_3 s'identifient à 3 invariants fondamentaux de φ de degrés 4, 8, 12. Définissons encore $p_4\in\mathbf{C}[V]^G_{1,5}$, $p_5\in\mathbf{C}[V]^G_{2,2}$, $p_6\in\mathbf{C}[V]^G_{2,6}$, $p_7\in\mathbf{C}[V]^G_{3,9}$ par

$$p_4(\varphi, \varphi')=(\varphi, \varphi'^5)_5,\ p_5(\varphi, \varphi')=(\psi_2, \varphi'^2)_2,\ p_6=(\psi_1, \varphi'^6)_6,\ p_7=(\psi_3, \varphi'^9)_9.$$

5. Théorème. (i) *Les éléments* $p_1, p_5, p_4, p_2+p_6, p_3+p_7$ *de* $\mathbf{C}[V]^G$ *sont homogènes pour la graduation totale, de degrés* 4, 4, 6, 8, 12.

(ii) *L'ensemble* $\{p_1, p_5, p_4, p_2+p_6, p_3+p_7\}$ *est un système de paramètres pour* $\mathbf{C}[V]^G$.

(iii) *La complexité de* $\mathbf{C}[V]^G$ *est* 38.

(iv) *Il n'existe pas de système de paramètres homogènes de* $\mathbf{C}[V]^G$ *correspondant à l'écriture* (1) *de la série de Poincaré.*

(i) est évident.

(ii) Supposons que $p_1, p_5, p_4, p_2+p_6, p_3+p_7$ s'annulent pour (φ, φ'). On va prouver que (φ, φ') est instable. Comme le degré de transcendance de $\mathbf{C}[V]^G$ sur $\mathbf{C}$ est 5, cela établira (ii).

Supposons d'abord $\psi_2=0$, donc $p_2=0$. D'après le lemme 3, on se ramène au cas où $\varphi=ax^5+5bx^4y$. Alors

$$\psi_1 = (ax^3+3bx^2y)\cdot 0-(bx^3)^2 = -b^2x^6,\ p_6 = -b^2b'^6,\ p_4 = ab'^5-5ba'b'^4.$$

Les conditions $p_4(\varphi, \varphi')=(p_2+p_6)(\varphi, \varphi')=0$ donnent $ab'^5-5ba'b'^4=b^2b'^6=0$. Si $b'=0$, (φ, φ') est instable d'après le critère de Hilbert—Mumford. Supposons $b'\neq 0$. Alors, $b=0$, puis $a=0$, donc $\varphi=0$ et il est clair que (φ, φ') est instable.

Supposons désormais $\psi_2\neq 0$. Puisque $0=p_1(\varphi, \varphi')=(\psi_2, \psi_2)_2$, ψ_2 admet une racine double en x/y, et, par action de $SL(2, \mathbf{C})$, on peut supposer que cette racine est 0. D'après le lemme 3, on a alors

$$ae-4bd+3c^2 \neq 0, \tag{3}$$

$$af-3be+2cd = 0, \tag{4}$$

$$bf-4ce+3d^2 = 0. \tag{5}$$

Par ailleurs, $0=p_5(\varphi, \varphi')=(ae-4bd+3c^2)b'^2$ donc, compte tenu de (3),

$$b' = 0. \tag{6}$$

Supposons d'abord $a'=0$. Alors p_6 et p_7, qui sont de degrés >0 en (a', b'), s'annulent pour (φ, φ'). Donc $0=p_1(\varphi)=p_2(\varphi)=p_3(\varphi)$ de sorte que φ est instable dans V_5. Alors $(\varphi, \varphi')=(\varphi, 0)$ est instable dans V.

Supposons désormais $a'\neq 0$. On a $0=p_4(\varphi, \varphi')=(\varphi, \varphi'^5)_5=-fa'^5$ donc

$$f = 0. \tag{7}$$

Comme ψ_2^5 est proportionnel à x^{10}, la condition (7) entraîne que $(\psi_2^5, \varphi^2)_{10}=0$, d'où $p_3(\varphi, \varphi')=0$. Alors, $p_7(\varphi, \varphi')=0$, c'est-à-dire $(\psi_3, \varphi'^9)_9=0$. Comme $\varphi'^9=a'^9x^9$, le seul terme de ψ_3 qui intervient dans le calcul de $(\psi_3, \varphi'^9)_9$ est le terme en y^9. Il nous suffit donc de considérer les termes en xy^4 et y^5 dans φ, en xy^5 et y^6 dans ψ_1:

$$\varphi = \ldots+5exy^4+fy^5 = \ldots+5exy^4,$$

$$\psi_1 = (\ldots+dy^3)(\ldots+3exy^2)-(\ldots+3dxy^2+ey^3)^2 = \ldots-3edxy^5-e^2y^6,$$

$$\psi_3 = (\ldots+ey^4)(\ldots-e^2y^5)-(\ldots+4exy^3)\left(\ldots-\frac{3}{6}edy^4\right).$$

Le terme en y^9 de ψ_3 est donc $-e^3y^9$, d'où $0=(\psi_3, \varphi'^9)_9=e^3a'^9$. Comme $a'\neq 0$, on en déduit que

$$e = 0. \tag{8}$$

Les conditions (5), (7), (8) donnent $d=0$. Comme $b'=0$, (φ, φ') est instable dans V d'après le critère de Hilbert—Mumford.

(iii) et (iv). Soit $(q_1, q_2, q_3, q_4, q_5)$ un système de paramètres homogènes de $\mathbf{C}[V]^G$. Soit $d_i=\deg(q_i)$. On peut supposer que $d_1\leqq d_2\leqq d_3\leqq d_4\leqq d_5$. Montrons que

$$d_1d_2d_3d_4d_5 \geqq 2^{10}\cdot 3^2. \tag{9}$$

On a

$$F(z) = \frac{A(z)}{(1-z^{d_1})(1-z^{d_2})(1-z^{d_3})(1-z^{d_4})(1-z^{d_5})}$$

où les coefficients du polynôme $A(z)$ sont $\geqq 0$. Nous allons imiter le raisonnement de [2], §2. D'après la forme irréductible (1), $F(z)$ admet -1 comme pôle d'ordre 5, $\sqrt{-1}$ comme pôle d'ordre 3, $(1+\sqrt{-3})/2$ comme pôle d'ordre 2. Donc les d_i sont tous pairs, trois d'entre eux sont divisibles par 4, deux d'entre eux sont divisibles par 6. Le développement en série de $F(z)$ commence par $1+2z^4+3z^6$. Comme les coefficients de $A(z)$ sont $\geqq 0$, on voit que les d_i sont tous $\geqq 4$, et que, si l'on note α (resp. β) le nombre de d_i égaux à 4 (resp. 6), on a $\alpha\leqq 2$, $\beta\leqq 3$.

Supposons $\alpha=0$. Les d_i sont $\geqq 6$. Trois d'entre eux sont divisibles par 4, donc trois d'entre eux sont $\geqq 8$. Donc $\prod d_i\geqq 8^3\cdot 6^2=2^{11}\cdot 3^2$. Supposons $\alpha=1$. Alors $d_1=4$. Les entiers d_2, d_3, d_4, d_5 sont $\geqq 6$ et deux d'entre eux sont $\geqq 8$, donc $\prod d_i\geqq 4\cdot 8^2\cdot 6^2=2^{10}\cdot 3^2$. Supposons $\alpha=2$. Alors $d_1=d_2=4$. Distinguons plusieurs cas. Supposons $\beta=0$. Alors $d_3\geqq 8$. Comme deux des d_i sont divisibles par 6, deux des d_i sont $\geqq 12$, donc $\prod d_i\geqq 4^2\cdot 8\cdot 12^2=2^{11}\cdot 3^2$. Supposons $\beta=1$. Alors $d_3=6$, $d_4\geqq 8$. Comme deux des d_i sont divisibles par 6, on a $d_5\geqq 12$, donc $\prod d_i\geqq 4^2\cdot 6\cdot 8\cdot 12=2^{10}\cdot 3^2$. Supposons $\beta=3$. Alors $d_3=d_4=d_5=6$, ce qui est impossible puisque trois des d_i sont divisibles par 4.

Reste le cas $\beta=2$. Alors $d_3=d_4=6$, $d_5\geqq 8$. Comme trois des d_i sont divisibles par 4, on a $d_5\in\{8, 12, 16, \ldots\}$. Si $d_5\geqq 16$, on a $\prod d_i\geqq 4^2\cdot 6^2\cdot 16=2^{10}\cdot 3^2$. On va enfin montrer que les cas $d_5=8$, $d_5=12$ sont impossibles. Supposons $d_5=8$. On aurait donc un système de paramètres homogènes de degrés 4, 4, 6, 6, 8. Les conditions $q_1(\varphi, 0)=q_2(\varphi, 0)=\ldots=q_5(\varphi, 0)=0$ doivent entraîner l'instabilité de φ. Or $\mathbf{C}[V_5]^G$ ne contient que deux éléments homogènes algébriquement indépendants de degré $\leqq 8$, et l'annulation pour φ de deux tels invariants ne peut entraîner l'instabilité de φ puisque $\mathbf{C}[V_5]^G$ a pour degré de transcendance 3. Supposons $d_5=12$. On aurait donc un système de paramètres homogènes de degrés 4, 4, 6, 6, 12.

Considérons leurs restrictions à V_5. Comme $\mathbf{C}[V_5]_6^G=0$ et que $\dim \mathbf{C}[V_5]_4^G=1$, on obtient une contradiction comme dans le cas précédent.

On a donc prouvé (9). Comme le produit $4^2\cdot 6^2\cdot 8=2^9\cdot 3^2$ correspondant à l'écriture (1) de $F(z)$ est $<2^{10}\cdot 3^2$, on en déduit (iv). D'autre part, l'écriture de $F(z)$ correspondant au système de paramètres trouvé en (ii) donne $\prod d_i=$ $=4^2\cdot 6\cdot 8\cdot 12=2^{10}\cdot 3^2$, et fournit donc la valeur minimale de $\prod d_i$ pour tous les systèmes de paramètres homogènes; dans cette écriture, le numérateur $A(z)$ se déduit du numérateur de (1) en multipliant par $1+z^6$; la somme des coefficients de $A(z)$ est alors

$$2(1+1+6+3+6+1+1) = 38$$

ce qui prouve (iii).

6. Il reste à savoir si l'on peut obtenir un contre-exemple analogue à 5 (iv) quand on considère une représentation *irréductible* de $SL(2, \mathbf{C})$. Cela est intéressant puisque les séries de Poincaré ont alors été calculées explicitement jusqu'à la dimension 17.

7. Le système de paramètres construit en 5 (ii) n'est pas bihomogène. En fait, il résulte de [1] qu'il n'existe aucun système de paramètres bihomogènes de $\mathbf{C}[V]^G$.

Deuxième partie

8. Lemme. *Soient n et p des entiers tels que $2\leqq p\leqq n$. On considère une forme binaire de degré n en x et y du type suivant:*

$$f(x, y) = a_0x^{n-u}y^u+a_1x^{n-u-p}y^{u+p}+a_2x^{n-u-2p}y^{u+2p}+\ldots+a_sx^{n-u-sp}y^{u+sp}$$

où $a_0, a_1, \ldots, a_s\in\mathbf{C}$. On suppose f instable. Alors $f(x, y)$ admet 0 ou ∞ comme racine en x/y de multiplicité $>n/2$.

Posons $g(X, Y)=a_0X^s+a_1X^{s-1}Y+a_2X^{s-2}Y^2+\ldots+a_sY^s$. On a $f(x, y)=$ $=x^{n-u-sp}y^ug(x^p, y^p)$. On considère les racines en X/Y de $g(X, Y)$, à l'exclusion de 0 et ∞; soient $\omega_1, \ldots, \omega_r$ ces racines, deux à deux distinctes; la somme de leurs multiplicités est $\leqq s$. Alors les racines en x/y de $f(x, y)$, à l'exclusion de 0 et ∞, sont

$$(\omega_j^{1/p}, \omega_j^{1/p}\exp(2i\pi/p), \ldots, \omega_j^{1/p}\exp(2i\pi(p-1)/p) \quad (j = 1, 2, \ldots, r).$$

Comme $\omega_j\neq 0, \infty$ pour tout j, chacune de ces racines est de multiplicité $\leqq s$. Or $u+sp\leqq n$, donc $s\leqq n/p\leqq n/2$. Comme f est instable, f admet une racine en x/y d'ordre $>n/2$. D'après ce qui précède, cette racine est 0 ou ∞.

9. Lemme. *Soient n, b des entiers $\geqq 1$. Soit p un nombre premier tel que $n/(2b-1)>p\geqq n/(2b+1)$. Soit $(P_1, P_2, \ldots, P_{n-2})$ un système de paramètres homo-*

gènes pour les formes binaires de degré n. Soit $\delta_j=\deg P_j$. *Alors p divise* δ_j *pour au moins b indices j.*

Toute forme binaire de degré n s'écrit $\alpha_0x^n+\alpha_1x^{n-1}y+\ldots+\alpha_ny^n$. Chaque P_j est un polynôme en $\alpha_0, \alpha_1, \ldots, \alpha_n$. Nous supposerons que $\delta_1, \ldots, \delta_r$ sont divisibles par p et que $\delta_{r+1}, \ldots, \delta_{n-2}$ sont non divisibles par p. Il s'agit de prouver que $r\geqq b$. Distinguons 4 cas suivant que $n/(2b-1)>p>n/2b$, $p=n/2b$, $n/2b>p>n/(2b+1)$, $p=n/(2b+1)$,

Dans le 1 er cas, on a

$$0<p<2p<\ldots<(b-1)p<n/2<bp<(b+1)p<\ldots<(2b-1)p<n. \tag{10}$$

Considérons une forme binaire du type suivant:

$$f(x,y)=\alpha_0x^n+\alpha_px^{n-p}y^p+\alpha_{2p}x^{n-2p}y^{2p}+\ldots+\alpha_{(2b-1)p}x^{n-(2b-1)p}y^{(2b-1)p}.$$

Supposons $P_{r+1}(f)\neq0$. Alors P_{r+1} contient, avec un coefficient non nul, un monôme de la forme

$$\alpha_0^{\mu_0}\alpha_p^{\mu_p}\alpha_{2p}^{\mu_{2p}}\alpha_{(2b-1)p}^{\mu_{(2b-1)p}}.$$

D'après [3], p. 32, on a $2(p\mu_p+2p\mu_{2p}+\ldots+(2b-1)p\mu_{(2b-1)p})=n\delta_{r+1}$. Comme p est premier et ne divise pas n, p divise δ_{r+1}, ce qui est absurde. Donc, $P_{r+1}(f)=0$. De même, $P_{r+2}(f)=\ldots=P_{n-2}(f)=0$.

Dans $P_1, \ldots, P_r$, remplaçons α_k par 0 toutes les fois que p ne divise pas k. On obtient des polynômes homogènes $Q_1, \ldots, Q_r$ en $\alpha_0, \alpha_p, \ldots, \alpha_{(2b-1)p}$. Les conditions

$$Q_1(\alpha_0, \ldots, \alpha_{(2b-1)p})=Q_2(\alpha_0, \ldots, \alpha_{(2b-1)p})=\ldots=Q_r(\alpha_0, \ldots, \alpha_{(2b-1)p})=0 \tag{11}$$

entraînent que $P_1(f)=\ldots=P_r(f)=0$. Par ailleurs, $P_{r+1}(f)=\ldots=P_{n-2}(f)=0$ comme on l'a vu. Donc f est instable. D'après (10) et le lemme 8, on a $\alpha_0=\alpha_p=\ldots=\alpha_{(b-1)p}=0$, ou $\alpha_{bp}=\alpha_{(b+1)p}=\ldots=\alpha_{(2b-1)p}=0$. Ainsi, les équations (11) définissent dans $\mathbf{C}^{2b}$ un cône algébrique de codimension $\geqq b$. Donc $r\geqq b$.

Dans le 2ème cas, on a

$$\begin{aligned}1<p+1<2p+1<\ldots<(b-1)p+1<n/2<bp+1<\\<(b+1)p+1<\ldots<(2b-1)p+1<n.\end{aligned} \tag{12}$$

Considérons une forme binaire du type suivant :

$$f(x,y)=\alpha_1x^{n-1}y+\alpha_{p+1}x^{n-p-1}y^{p+1}+\ldots+\alpha_{(2b-1)p+1}x^{n-(2b-1)p-1}y^{(2b-1)p+1}.$$

Si $P_{r+1}(f)\neq0$, on voit comme dans le 1 er cas qu'il existe des entiers μ_j tels que

$$2(\mu_1+(p+1)\mu_{p+1}+(2p+1)\mu_{2p+1}+\ldots+((2b-1)p+1)\mu_{(2b-1)p+1})=n\delta_{r+1}=2bp\delta_{r+1},$$

$$\mu_1+\mu_{p+1}+\mu_{2p+1}+\ldots+\mu_{(2b-1)p+1}=\delta_{r+1}$$

d'où $p\mu_{p+1}+2p\mu_{2p+1}+\ldots+(2b-1)p\mu_{(2b-1)p+1}=(bp-1)\delta_{r+1}$. Donc p divise δ_{r+1}, ce qui est absurde. Donc $P_{r+1}(f)=P_{r+2}(f)=\ldots=P_{n-2}(f)$.

Dans $P_1, \ldots, P_r$, remplaçons α_k par 0 toutes les fois que $k\notin\{1, p+1, 2p+1, \ldots, (2b-1)p+1\}$. On obtient des polynômes $Q_1, \ldots, Q_r$ dont l'annulation entraîne l'instabilité de f. D'après (12) et le lemme 8, on a $r\geqq b$.

Dans le 3ème cas, on a

$$0<p<2p<\ldots<bp<n/2<(b+1)p<(b+2)p<\ldots<2bp<n.$$

On considère $\alpha_0x^n+\alpha_px^{n-p}y^p+\ldots+\alpha_{2bp}x^{n-2bp}y^{2bp}$ et l'on raisonne comme dans le 1er cas.

Dans le 4ème cas, et si $p>2$, on a

$$1<p+1<2p+1<\ldots<bp+1<n/2<(b+1)p+1<\ldots<2bp+1<n.$$

Raisonnant comme dans le 2ème cas, on a cette fois

$$2(\mu_1+(p+1)\mu_{p+1}+\ldots+(2bp+1)\mu_{2bp+1})=(2b+1)p\delta_{r+1},$$

$$\mu_1+\mu_{p+1}+\ldots+\mu_{2bp+1}=\delta_{r+1}$$

d'où $2(p\mu_{p+1}+2p\mu_{2p+1}+\ldots+2bp\mu_{2bp+1})=((2b+1)p-2)\delta_{r+1}$. Comme $p>2$, p divise δ_{r+1} et l'on termine comme plus haut. Supposons $p=2$, donc $n=2(2b+1)$. On revient à la méthode du 1er cas, en écrivant

$$0<2<4<\ldots<2b<n/2<2b+2<\ldots<4b+2=n,$$

$$f(x, y)=\alpha_0x^n+\alpha_2x^{n-2}y^2+\alpha_4x^{n-4}y^4+\ldots+\alpha_ny^n.$$

Si $P_{r+1}(f)\neq0$, on a $2(2\mu_2+4\mu_4+\ldots+n\mu_n)=2(2b+1)\delta_{r+1}$ donc 2 divise δ_{r+1}, ce qui est absurde. On trouve même, dans ce cas, que p divise δ_j pour au moins $b+1$ indices j.

10. Théorème. *Soit A un nombre $<1/2$. Alors $c_n\geqq\exp(An\log n)$ pour n assez grand.*

Soit $p_1>p_2>\ldots$ la suite décroissante des nombres premiers $<n$. Soit $a=a_n$ le plus petit entier $\geqq0$ tel que $n/(2a+1)<2$. Définissons des entiers $s_1, s_2, \ldots, s_a$ par

$$n>p_1>p_2>\ldots>p_{s_1}\geqq n/3$$

$$n/3>p_{s_1+1}>p_{s_1+2}>\ldots>p_{s_2}\geqq n/5$$

$$n/5>p_{s_2+1}>p_{s_2+2}>\ldots>p_{s_3}\geqq n/7$$

$$\vdots$$

$$n/(2a-1)>p_{s_{a-1}+1}>p_{s_{a-1}+2}>\ldots>p_{s_a}\geqq n/(2a+1)$$

(certaines lignes de ce tableau peuvent ne contenir aucun p_i).

Pour $p=p_{s_{b-1}+1}, p_{s_{b-1}+2}, \ldots, p_{s_b}$, p^b divise $\delta_1\delta_2\ldots\delta_{n-2}$ (lemme 9). Par suite,

$$\delta_1\delta_2 \ldots \delta_{n-2} \geqq p_1 p_2 \cdots p_{s_1} p_{s_1+1}^2 p_{s_1+2}^2 \cdots p_{s_2}^2 \cdots p_{s_{a-1}+1}^a p_{s_{a-1}+2}^a \cdots p_{s_a}^a$$

ou

$$\delta_1\delta_2 \ldots \delta_{n-2} \geqq (p_1 p_2 \cdots p_{s_a})(p_{s_1+1} p_{s_1+2} \cdots p_{s_a}) \cdots (p_{s_{a-1}+1} p_{s_{a-1}+2} \cdots p_{s_a}).$$

Soit $\mathscr{P}$ l'ensemble des nombres premiers. Pour x réel tendant vers $+\infty$, on a $\log \prod_{p\in\mathscr{P}, p<x} p \sim x$ ([5], th. 413 et 434). Choisissons des nombres A', A'' tels que $2A<A''<A'<1$. Soit $d=d_n$ le plus petit entier tel que $2d-1\geqq n/\log n$. On a, pour n assez grand,

$$\prod_{\substack{p\in\mathscr{P}\\ p<n}} p \geqq \exp(A'n), \quad \prod_{\substack{p\in\mathscr{P}\\ p<n/3}} p \geqq \exp\left(A'\frac{n}{3}\right), \ldots, \prod_{\substack{p\in\mathscr{P}\\ p<n/(2d-1)}} p \geqq \exp\left(A'\frac{n}{2d-1}\right)$$

donc

$$\delta_1\delta_2 \ldots \delta_{n-2} \geqq \exp\left(A'n\left(1+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{2d-1}\right)\right).$$

Quand $n\to\infty$, on a $d\sim n/2\log n$, donc

$$1+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{2d-1} \sim \frac{1}{2}\log\frac{n}{\log n} \sim \frac{1}{2}\log n.$$

Par suite, pour n assez grand, on a

$$\delta_1\delta_2 \ldots \delta_{n-2} \geqq \exp\left(\frac{1}{2}A''n\log n\right). \tag{13}$$

Si le système de paramètres $(P_1, \ldots, P_{n-2})$ est choisi convenablement, on a

$$c_n/(\delta_1\delta_2 \ldots \delta_{n-2}) \geqq Bn^{-9/2} \tag{14}$$

où B est une constante >0 ([6], 3.4.12). Le théorème résulte de (13) et (14).

11. Remarque. Il est probable qu'en fait la croissance de c_n est encore plus rapide.

12. Remarque. En considérant dans le lemme 9 des puissances de nombres premiers, on peut améliorer légèrement la conclusion de ce lemme. Mais cela ne permet pas d'améliorer le théorème 10.

Bibliographie

[1] M. Brion, Invariants de plusieurs formes binaires, *Bull. Soc. Math. France*, **110** (1982), 429—445.

[2] J. Dixmier, Série de Poincaré et systèmes de paramètres pour les invariants des formes binaires de degré 7, *Bull. Soc. Math. France*, **110** (1982), 303—318.

[3] E. B. Elliott, *An introduction to the algebra of quantics*, 2nd ed., Oxford Univ. Press (1913).

[4] J. H. Grace and A. Young, *The algebra of invariants*, Cambridge Univ. Press (1903).

[5] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford Univ. Press (1960).

[6] T. A. Springer, *Invariant theory*, Lecture Notes in Mathematics, vol. 585, Springer-Verlag (Berlin, 1977).

[7] R. P. Stanley, Hilbert functions of graded algebras, *Adv. in Math.*, **28** (1978), 57—83.

[8] J. J. Sylvester and F. Franklin, Tables of generating functions and grundforms for the binary quantics of the first ten orders, *Amer. J. Math.*, **2** (1879), 223—251.

LABORATOIRE DE MATHÉMATIQUES FONDAMENTALES
UNIVERSITÉ PIERRE ET MARIE CURIE
4 PLACE JUSSIEU
75230 PARIS CEDEX 05, FRANCE